(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－328120

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｄ
	1/00	３７０		1/00	３７０Ｅ
	12/00	５３７		12/00	５３７Ａ
	12/14	３２０		12/14	３２０Ｃ

審査請求　有　　請求項の数６　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－137928

(22)出願日　平成10年(1998)５月20日

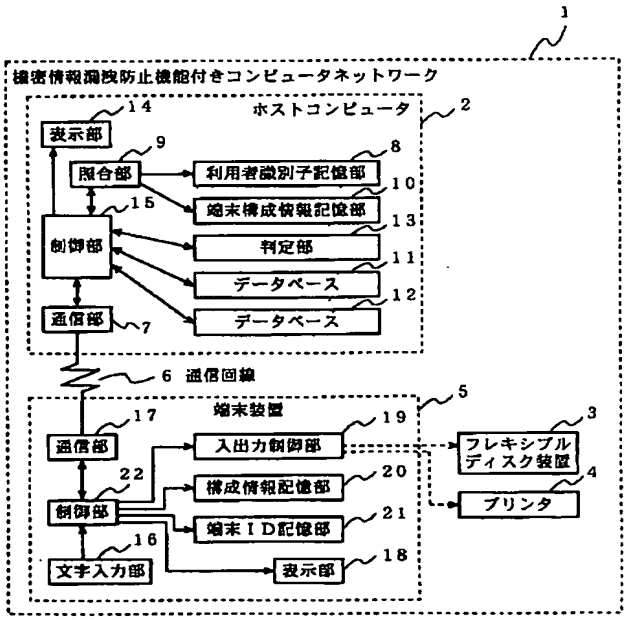
(71)出願人　000232140
日本電気フィールドサービス株式会社
東京都港区三田１丁目４番28号
(72)発明者　内倉　紀之
東京都港区三田一丁目４番28号　日本電気フィールドサービス株式会社内
(74)代理人　弁理士　岩佐　義幸

(54)【発明の名称】　機密情報漏洩防止機能付きコンピュータネットワーク

(57)【要約】

【課題】　端末装置の入出力機器の構成や利用者プログラムによって、データベースへのアクセス権を設定することにより、データベース内の機密情報の漏洩を防止する。

【解決手段】　ホストコンピュータ２は端末装置５からの通信要求を受けると、照合部９にて利用者識別子記憶部８に登録されている利用者識別子との照合を行い、照合結果が一致すると、端末装置５へ構成情報を要求する。端末装置５から構成情報を受信すると、照合部９にて端末構成情報記憶部１０に記憶されている構成情報と照合を行い、照合結果が一致すると、端末装置５のデータベース１１，１２へのアクセス権の有無を判定部１３に行わせる。判定部１３から判定結果をうけた制御部１５は以後、端末装置５にアクセス権の有るデータベースの使用を許可する。



【特許請求の範囲】
【請求項１】端末装置には該端末装置の端末構成情報を記憶し、また該端末装置が接続されるホストコンピュータには端末装置ごとの利用者識別子および端末構成情報を記憶しておき、通信要求を受信したホストコンピュータは、当該端末装置から受信した利用者識別子および端末構成情報と自らが記憶している利用者識別子および端末構成情報とを照合して一致したときに、当該端末装置に対してデータベースへのアクセスの許否を判定するようにしたことを特徴とする機密情報漏洩防止機能付きコンピュータネットワーク。
【請求項２】前記端末構成情報は、当該端末装置を構成する入出力機器の構成を示す情報であることを特徴とする請求項１記載の機密情報漏洩防止機能付きコンピュータネットワーク。
【請求項３】前記端末装置は、前記利用者識別子のうちの端末ＩＤを記憶している端末ＩＤ記憶部と、前記端末構成情報を記憶している構成情報記憶とを有し、
また、前記ホストコンピュータは、前記端末ＩＤ，利用者ＩＤおよびパスワードを含む利用者識別子を記憶している利用者識別子記憶部と、前記端末ＩＤごとに前記入出力機器の有無を示す端末構成情報を記憶している端末構成情報記憶部と、前記利用者識別子および前記端末構成情報の照合を行う照合部と、該照合の結果により一致したときに当該端末装置の各入出力機器に対するデータベースごとのアクセス権の有無を判定する判定部とを有することを特徴とする請求項２記載の機密情報漏洩防止機能付きコンピュータネットワーク。
【請求項４】前記端末構成情報は、当該端末装置に格納された利用者プログラムを示す情報であることを特徴とする請求項１記載の機密情報漏洩防止機能付きコンピュータネットワーク。
【請求項５】前記端末装置は、前記利用者識別子のうちの端末ＩＤを記憶している端末ＩＤ記憶部と、前記利用者プログラムを格納する利用者プログラム格納部と、前記ホストコンピュータから要求されると前記利用者プログラム格納部を検索する利用者プログラム検索部とを有し、
また、前記ホストコンピュータは、前記端末ＩＤ，利用者ＩＤおよびパスワードを含む利用者識別子を記憶している利用者識別子記憶部と、前記端末ＩＤごとに前記利用者プログラムの有無を示す端末構成情報を記憶している端末構成情報記憶部と、前記利用者識別子および前記端末構成情報の照合を行う照合部と、該照合の結果により一致したときに当該端末装置の各利用者プログラムに対するデータベースごとのアクセス権の有無を判定する判定部とを有することを特徴とする請求項４記載の機密情報漏洩防止機能付きコンピュータネットワーク。
【請求項６】前記端末構成情報の照合の結果により、不一致が検出されたときは、当該端末装置の端末構成が変更されたことを表示することを特徴とする請求項１～請求項５のいずれかに記載の機密情報漏洩防止機能付きコンピュータネットワーク。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、機密情報漏洩防止機能付きコンピュータネットワークに関する。
【０００２】
【従来の技術】従来、コンピュータネットワークの機密情報漏洩防止は、利用者識別コード毎のアクセス権にセキュリティを設ける方式、および利用者識別コードと端末識別コードの整合性を確認する方式により行われている。
【０００３】たとえば、特開平５－６１８３４号公報には、オンライン接続時に端末・利用者整合性をチェックする手段を設けることにより、機密情報の漏洩を防止する技術が記載されている。図７は、この従来の機密情報漏洩防止方式の一例を示すブロック図である。通信回線５１，５２によりホストコンピュータ５３と接続された端末５４，５５から、利用者５４，５５がデータベース５８，５９を利用するデータベースシステムにおいて、ホストコンピュータ５３には、データベース利用プログラム６０と、利用者識別コードに対して利用できるデータベース資源の範囲と利用方法とを制限する資源管理手段６１とに加え、使用している端末と入力された利用者識別コードとの整合性を確認する端末・利用者整合性チェック手段６２を備えている。
【０００４】以下、図８のフローチャートを参照しながら図７の実施例の動作を説明する。ここで、利用者５６にはデータベース５８の参照権があり、利用する端末は端末５４であるとし、利用者５７はシステム管理者で、利用する端末は端末５５であるとする。
【０００５】まず、利用者５６が端末５４を使用したときの動作を示す。利用者５６がコンピュータ５３に回線接続を要求すると、ホストコンピュータ５３は端末５４が送出する端末識別コードから登録された端末であることを確認し、利用者識別コードの送信を要求する（ステップ１０１）。利用者５６が端末５４のキーボードから自分の利用者識別コードを入力すると（ステップ１０２）、利用者識別コードが登録済みであるか否かをチェックし、登録済みの場合は端末識別コードと利用者識別コードとを端末・利用者整合性チェック手段６２に渡し、登録されていない場合は再入力を促す（ステップ１０３）。端末・利用者整合性チェック手段６２は、あらかじめ登録されている端末識別コードと利用者識別コードの組み合わせと照合し（ステップ１０４）、一致した組み合わせが無ければ整合性なしと判断してステップ１０２に戻り再度利用者識別コードの入力を要求するが、一致した組み合わせが有ればステップ１０６に進む（ステップ１０５）

【０００６】この例では、利用者５６と端末５４とは整合性があるので、ステップ１０６に進みデータベース利用プログラム６０の利用が開始される。データベース利用プログラム６０は、資源管理手段６１により利用者５６が使用するデータベースとその利用方法を制限する。すなわち、利用者５６の要求がデータベース５８の参照であれば、利用を許可するが、データベース５８の更新や、データベース５９の参照などは許可されない。

【０００７】次に、利用者５６が端末５５を使用したときの動作について示す。利用者５６の利用者識別コードも端末５５にも登録されているので、ホストコンピュータ５３に接続してステップ１０３までは進むが、端末・利用者整合性チェック手段６２により整合性なしと判定されるので、利用者５６は端末５５からはデータベースの利用ができないことになる。利用者５７が端末５４を使用するときも同様である。すなわち、端末５４を所有する利用者５６が、システム管理者である利用者５７の利用者識別コードを知り、端末５４から不正なデータベース利用を試みても、端末・利用者整合性チェック手段６２がそれを拒否することになる。

【０００８】利用者５７が端末５５を使用したときの動作は、利用者５７の利用者識別コードを端末５５から入力すると、端末・利用者整合性チェック手段６２により整合性が調べられるが、整合性があるのでデータベース利用プログラム６０が利用できる。データベース利用プログラム６０は、資源管理手段６１により利用者５７がシステム管理者であることを知らされ全資源の利用を許可することになる。

【０００９】

【発明が解決しようとする課題】しかしながら、上述した従来技術では、利用者５６，５７が使用している端末５４，５５自体の特定は容易であるため、利用者識別コードが漏洩することにより、第三者がたやすくデータベースに登録された情報を入手することができるようになるという問題点がある。

【００１０】本発明の目的は、端末構成情報によるチェックを介入させることにより、利用者識別子が第三者に漏洩した場合でも、データベース内の機密情報の漏洩を防止できる機密情報漏洩防止機能付きコンピュータネットワークを提供することにある。

【００１１】

【課題を解決するための手段】本発明の機密情報漏洩防止機能付きコンピュータネットワークは、端末装置には該端末装置の端末構成情報を記憶し、また該端末装置が接続されるホストコンピュータには端末装置ごとの利用者識別子および端末構成情報を記憶しておき、通信要求を受信したホストコンピュータは、当該端末装置から受信した利用者識別子および端末構成情報と自らが記憶している利用者識別子および端末構成情報とを照合して一致したときに、当該端末装置に対してデータベースへのアクセスの許否を判定するようにしたことを特徴とする。

【００１２】また、本発明の好ましい実施の形態としての機密情報漏洩防止機能付きコンピュータネットワークは、前記端末構成情報は、当該端末装置を構成する入出力機器の構成を示す情報であることを特徴とする。

【００１３】本発明の好ましい実施の形態としての機密情報漏洩防止機能付きコンピュータネットワークは、前記端末構成情報は、当該端末装置に格納された利用者プログラムを示す情報であることを特徴とする。

【００１４】本発明の好ましい実施の形態としての機密情報漏洩防止機能付きコンピュータネットワークは、前記端末構成情報の照合の結果により、不一致が検出されたときは、当該端末装置の端末構成が変更されたことを表示することを特徴とする。

【００１５】

【発明の実施の形態】次に、本発明の実施の形態について説明する。

【００１６】本発明の機密情報漏洩防止機能付きコンピュータネットワークは、端末装置には該端末装置の端末構成情報を記憶し、また該端末装置が接続されるホストコンピュータには端末装置ごとの利用者識別子および端末構成情報を記憶しておき、通信要求を受信したホストコンピュータは、当該端末装置から受信した利用者識別子および端末構成情報と自らが記憶している利用者識別子および端末構成情報とを照合して一致したときに、当該端末装置に対してデータベースへのアクセスの許否を判定するようにしたことを特徴とする。

【００１７】以下、本発明の実施例について図面を参照して説明する。

【００１８】本発明の一実施例を示す図１のブロック図を参照すると、本機密情報漏洩防止機能付きコンピュータネットワーク１は、ホストコンピュータ２と、入出力機器であるフレキシブルディスク装置３およびプリンタ４を接続可能な端末装置５と、ホストコンピュータ２と端末装置５を結ぶ通信回線６を含む。

【００１９】ホストコンピュータ２は、端末装置５との通信を行う通信部７と、端末装置５の利用者ＩＤとパスワードと端末ＩＤを記憶している利用者識別子記憶部８と、利用者識別子記憶部８に記憶されている利用者識別子と端末装置５から受信した利用者ＩＤ，パスワード，端末ＩＤ，端末構成情報の照合を行う照合部９と、端末装置５の端末構成情報を記憶している端末構成情報記憶部１０と、端末装置５から受信した入出力機器の構成情報によりデータベース１１、データベース１２へのアクセス権の有無を判定する判定部１３と、異常を検出した場合に管理者に通知する表示部１４と、通信部７，利用者識別子記憶部８，照合部９，端末構成情報記憶部１０，判定部１３および表示部１４を制御する制御部１５を含む。

【００２０】端末装置５は、利用者ＩＤとパスワードを入力する文字入力部１６と、ホストコンピュータ２との通信を行う通信部１７と、ホストコンピュータ２からの利用者ＩＤとパスワードの要求を利用者に通知する表示部１８と、端末装置５に接続された入出力機器の制御を行う入出力制御部１９と、入出力機器の構成情報を記憶する構成情報記憶部２０と、端末ＩＤを記憶する端末ＩＤ記憶部２１と、文字入力部１６，通信部１７，表示部１８，入出力制御部１９，構成情報記憶部２０および端末ＩＤ記憶部２１を制御する制御部２２を含む。

【００２１】次に、図１のブロック図、図２の流れ図を参照して本実施例の動作について詳細に説明する。

【００２２】利用者が端末装置５の使用を開始すると、制御部２２は通信部１７を経由してホストコンピュータ２に通信要求を送信する（図２のステップＡ１）。端末装置５からの通信要求を通信部７を経由して受信した制御部１５は、端末装置５に対して利用者ＩＤ，パスワードおよび端末ＩＤの利用者識別子の要求を行う（ステップＡ２）。

【００２３】ホストコンピュータ２から利用者ＩＤ，パスワード，端末ＩＤの要求を受信した制御部２２は、利用者に対して利用者ＩＤとパスワードの入力を促すメッセージを表示部１８に表示する（ステップＡ３）。この表示を見た利用者が利用者ＩＤとパスワードを入力すると、文字入力部１６から制御部２２に伝わり、制御部２２は、端末ＩＤ記憶部２１から端末ＩＤを読み出し、利用者ＩＤ，パスワードおよび端末ＩＤをホストコンピュータ２へ送信する（ステップＡ４）。

【００２４】利用者ＩＤ，パスワードおよび端末ＩＤを受信した制御部１５は、利用者識別子記憶部８に記憶されている利用者ＩＤ，パスワードおよび端末ＩＤとの照合を照合部９に行わせる（ステップＡ５）。照合部９から利用者ＩＤ，パスワードおよび端末ＩＤの照合結果を受けた制御部１５は、照合結果が一致している場合は端末装置５へ構成情報の要求を送信する（ステップＡ６）。照合結果が不一致の場合は端末装置５との通信を切断する（ステップＡ７）。

【００２５】ステップＡ６によりホストコンピュータ２から構成情報の要求を受けた制御部２２は、構成情報記憶部２０を参照し構成情報をホストコンピュータ２へ送信する（ステップＡ８）。

【００２６】端末装置３から構成情報を受信した制御部１５は、端末構成情報記憶部１０に記憶されている端末装置５の構成情報との照合を照合部７に行わせる（ステップＡ９）。照合部９から構成情報の照合結果を受けた制御部１５は、照合結果が一致している場合は端末装置５がデータベース１１，１２へのアクセス権の有無を判定部１３に行わせ（ステップＡ１１）、照合結果が一致していない場合は、端末装置５の構成情報が変更になったことを表示部１４に表示させ（ステップＡ１０）、端末装置５との通信を切断する（ステップＡ７）。これにより、端末の構成があらかじめ登録されたものとは異なっていることを管理者等に通知することができるようになる。

【００２７】ステップＡ１１において、判定部１３は端末装置５の構成により、データベース１１とデータベース１２へのアクセス権の有無を判定する。判定部１３から端末装置５のアクセス権の判定結果をうけた制御部１５は、以後、端末装置５にアクセス権のあるデータベースのみ使用を許可する（ステップＡ１２，Ａ１３）。本例では、膨大なデータ量のデータベース１１とそうでないデータベース１２とに分けてプリンタとフレキシブルディスク装置ごとにアクセス権を判定している。

【００２８】次に、具体例を用いて本実施例の動作を説明する。

【００２９】図３に示すように、例えば、利用者識別子記憶部８には、利用者ＩＤ「００Ａ１」、「００Ｂ２」、「００Ｃ３」とそのパスワードおよび端末ＩＤが登録されている。また、端末構成情報記憶部１０には、端末ＩＤ「Ｄ１」、「Ｅ１」、「Ｆ１」ごとにフレキシブルディスク装置およびプリンタの有無が登録されており、判定部１３には、フレキシブルディスク装置およびプリンタの有無によりデータベース１１，１２へのアクセス権の判定基準を備えているとする。判定部１３において、入出力機器が無いときデータベース１１，１２にアクセス権を認めてもその機密が漏洩することはなく、また、プリンタが有ってもデータベース１１にのみアクセス権を認めても膨大なデータ量のデータベース１１であればそれを印刷するのは至難であるとの判断による。

【００３０】いま、制御部１５からの要求に応えて、フレキシブルディスク装置３およびプリンタ４が接続されていない端末装置５からホストコンピュータ２へ利用者識別子“利用者ＩＤ「００Ａ１」，パスワード「００Ａ２」，端末ＩＤ「Ｄ１」”が、送信したとする（ステップＡ１からＡ４）。これらの利用者識別子は、利用者識別子記憶部８に登録されているので、照合部９による照合結果は一致となり、制御部１５は、端末装置５へ構成情報を要求する（ステップＡ５およびＡ６）。制御部２２は構成情報記憶部２０を参照し構成情報をホストコンピュータ２へ送信する。

【００３１】端末装置５から構成情報である「フレキシブルディスク装置無し」、「プリンタ無し」を受信した制御部１５は、端末構成情報記憶部１０に記憶されている端末ＩＤ「Ｄ１」の構成情報と一致しているため、端末装置５のデータベース１１，１２へのアクセス権の有無を判定部１３に行わせる（ステップＡ７，Ａ８およびＡ９）。端末装置５の構成情報は「フレキシブルディスク装置無し」、「プリンタ無し」であるから、判定部１３はデータベース１１とデータベース１２のアクセス権が有ると判定する（ステップＡ１１）。判定部１３から

判定結果をうけた制御部１５は以後、端末装置５のデータベース１１，１２使用を許可する（ステップＡ１３）。

【００３２】次に、本発明の他の実施例について図４～図６により説明する。図４を参照すると、本実施例は、図１に示された実施例における端末装置５に利用者プログラム検索部２３および利用者プログラム格納部２４が追加される点で異なる。

【００３３】利用者プログラム検索部２３は、利用者プログラム格納部２４の利用者プログラムを検索し検索結果を制御部２２に通知する。図５のステップＡ１～Ａ７で示される本実施例におけるホストコンピュータ２および端末装置５の各部の動作は、図１に示された実施例のホストコンピュータ２および端末装置５の各部の動作と同一のため、説明は省略する。また、以下の説明で構成情報というときは、利用者プログラム格納部２４に格納された利用者プログラムを指し、構成情報記憶部２０が記憶している入出力機器の構成は含めないものとする。

【００３４】ホストコンピュータ２から構成情報の要求を受けた制御部２２は、利用者プログラム検索部２３に利用者プログラム格納部２４の検索を行わせる。利用者プログラム検索部２３は利用者プログラム格納部２４に格納されたプログラムを検索し、検索結果を制御部２２に通知する。制御部２２は検索結果をホストコンピュータ２へ送信する（ステップＢ１およびＢ２）。

【００３５】端末装置５から構成情報を受信した制御部１５は、端末構成情報記憶部１０に記憶されている端末装置５の構成情報との照合を照合部９に行わせる（ステップＢ３）。照合部９から構成情報の照合結果を受けた制御部１５は、照合結果が一致している場合は端末装置５がデータベース１１，１２へのアクセス権の有無を判定部１３に行わせ（ステップＢ５）、照合結果が一致していない場合は、端末装置５の構成情報が変更になったことを表示部１４に表示させ、端末装置５との通信を切断する（ステップＢ４およびＡ７）。

【００３６】ステップＢ５において、判定部１３は端末装置５の構成情報によりデータベース１１とデータベース１２へのアクセス権の有無を判定する。判定部１３から端末装置５のアクセス権の判定結果をうけた制御部１５は以後、端末装置５にアクセス権のあるデータベースのみ使用を許可する（ステップＢ６およびＢ７）。なお、本例においては、データベース１１とデータベース１２とに分けて、プログラムの改ざんが許されているプログラムＡと許されていないプログラムＢごとにアクセス権を判定している。

【００３７】次に、具体例を用いて本実施例の動作を説明する。

【００３８】いま、利用者識別子記憶部８には、利用者ＩＤ「００Ａ１」、「００Ｂ２」、「００Ｃ３」とそのパスワードおよび端末ＩＤが登録されている。また、図６に示すように、端末構成情報記憶部１０には端末ＩＤ「Ｄ１」、「Ｅ１」、「Ｆ１」のプログラムＡおよびプログラムＢの有無が登録され、判定部１３にはプログラムＡおよびプログラムＢの有無によりデータベース１１，１２へのアクセス権の判定基準を備えている。加えて、端末装置５の利用者プログラム格納部２４にはデータベース１１，１２内のデータを変更できるプログラムＡが格納されているものとする。

【００３９】いま、利用者識別子“利用者ＩＤ「００Ａ１」，パスワード「００Ａ２」，端末ＩＤ「Ｄ１」”がプログラムＡを有する端末装置５から与えられたとする。これらの利用者識別子は利用者識別子記憶部８に登録されているので、照合部９の照合結果は一致となり、制御部１５は、端末装置５へ構成情報を要求する（ステップＡ１からＡ６）。構成情報の要求を受けた制御部２２は、利用者プログラム検索部２３に利用者プログラム格納部２４の検索を行わせる。利用者プログラム検索部２３は利用者プログラム格納部２４に格納されたプログラムＡを発見し、検索結果を制御部２２に通知する。制御部２２は検索結果をホストコンピュータ２へ送信する（ステップＢ１およびＢ２）。

【００４０】端末装置５から構成情報である「プログラムＡ有り」を受信した制御部１５は、端末構成情報記憶部１０に記憶されている端末ＩＤ「Ｄ１」の構成情報と一致しているため、端末装置５のデータベース１１，１２へのアクセス権の有無を判定部１３に行わせる（ステップＢ３）。端末装置５の構成情報は「プログラムＡ有り」であるから、判定部１３はデータベース１１のアクセス権が有ると判定する（ステップＢ５およびＢ６）。判定部１３から判定結果をうけた制御部１５は以後、端末装置５のデータベース１１の使用を許可する。

【００４１】

【発明の効果】第１の効果は、端末装置の入出力機器の構成や利用者プログラムによって、データベースのアクセス権限を設定できることにある。この結果、利用者識別子が第三者に漏洩した場合でも、データベース内の機密情報の漏洩が防止できる。その理由は、機密情報が格納されたデータベースのアクセス権を入出力機器の無い端末やアクセス権を認めても支障のない入出力機器や利用者プログラムにのみ与えることにより、機密情報を記録して外部に持ち出したり、データベースにアクセスすることができないためである。

【００４２】第２の効果は、管理者が端末装置の入出力機器の構成や利用者プログラムを管理できることにある。その理由は、端末装置の入出力機器の構成や利用者プログラムが、あらかじめ登録された構成と異なる場合に、管理者に通知する手段を備えたためである。

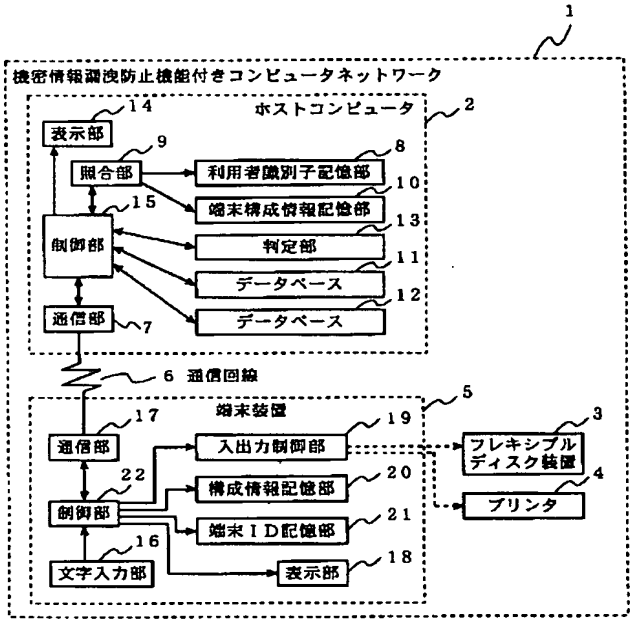
【図面の簡単な説明】

【図１】本発明の一実施例のブロック図

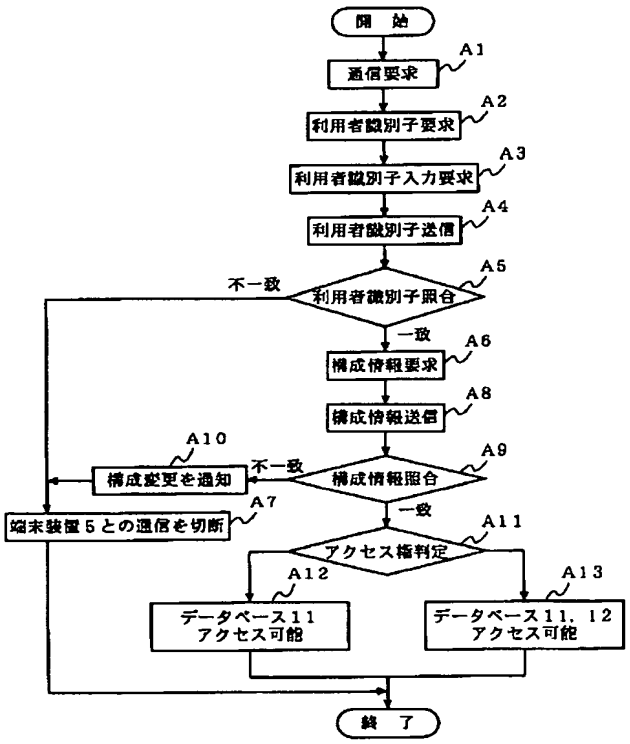
【図２】図１に示した実施例の

【図３】図１に示し多実施例の動作を具体例により説明するための図
【図４】本発明の他の実施例のブロック図
【図５】図４に示した実施例のフローチャート
【図６】図４に示した実施例の動作を具体例により説明するための図
【図７】従来例のブロック図
【図８】図７に示した従来例のフローチャート
【符号の説明】
１　機密情報漏洩防止機能付きコンピュータネットワーク
２，５３　ホストコンピュータ
３　フレキシブルディスク装置
４　プリンタ
５，５０　端末装置
６，５１，５２　通信回線
７，１７　通信部
８　利用者識別子記憶部
９　照合部
１０　端末構成情報記憶部
１１，１２，５８，５９　データベース
１３　判定部
１４，１８　表示部
１５，２２　制御部
１６　文字入力部
１９　入出力制御部
２０　構成情報記憶部
２１　端末ＩＤ記憶部
２３　利用者プログラム検索部
２４　利用者プログラム格納部
５４，５５　端末
５６，５７　利用者
６０　データベース利用者プログラム
６１　資源管理手段
６２　端末・利用者整合性チェック手段

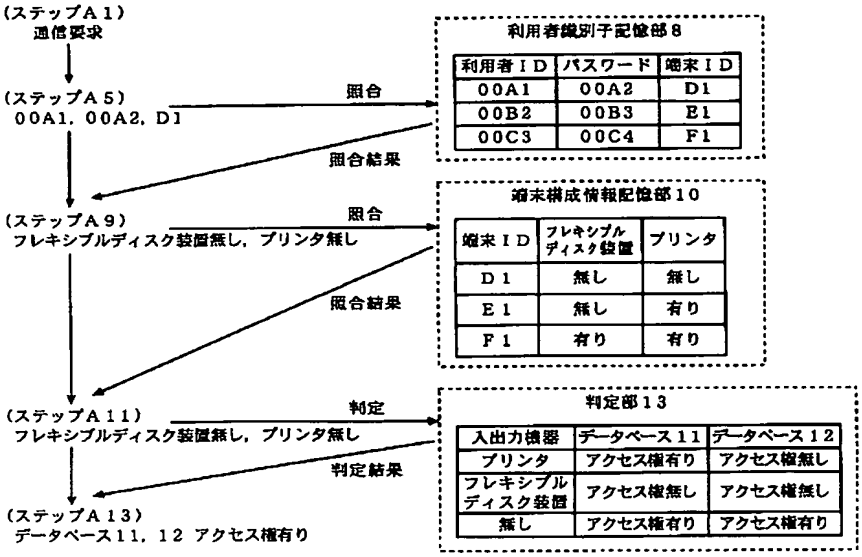
【図１】



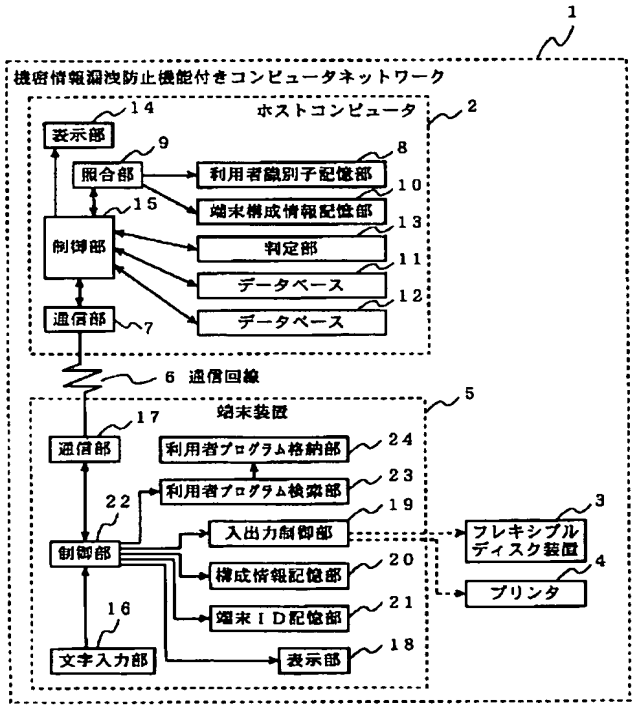
【図２】



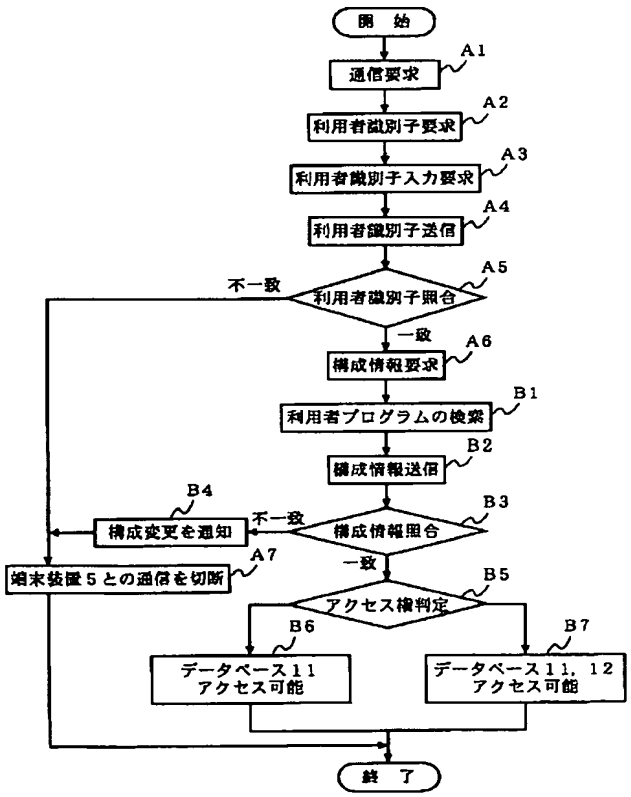
【図３】


（ステップＡ１）
通信要求
（ステップＡ５）
００Ａ１，００Ａ２，Ｄ１
照合
照合結果
利用者識別子記憶部８
利用者ＩＤ | パスワード | 端末ＩＤ
００Ａ１ | ００Ａ２ | Ｄ１
００Ｂ２ | ００Ｂ３ | Ｅ１
００Ｃ３ | ００Ｃ４ | Ｆ１
（ステップＡ９）
フレキシブルディスク装置無し，プリンタ無し
照合
照合結果
端末構成情報記憶部１０
端末ＩＤ | フレキシブルディスク装置 | プリンタ
Ｄ１ | 無し | 無し
Ｅ１ | 無し | 有り
Ｆ１ | 有り | 有り
（ステップＡ１１）
フレキシブルディスク装置無し，プリンタ無し
判定
判定結果
判定部１３
入出力機器 | データベース１１ | データベース１２
プリンタ | アクセス権有り | アクセス権無し
フレキシブルディスク装置 | アクセス権無し | アクセス権無し
無し | アクセス権有り | アクセス権有り
（ステップＡ１３）
データベース１１，１２ アクセス権有り

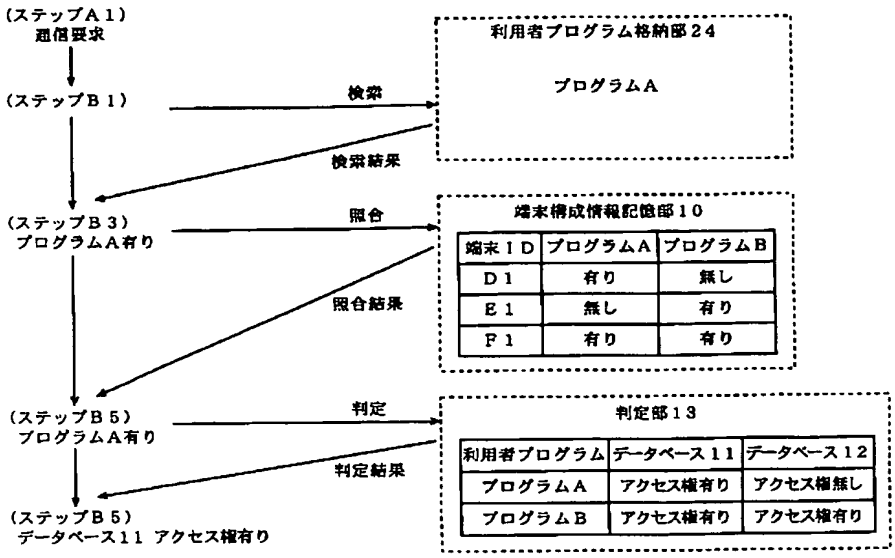
【図４】


1
機密情報漏洩防止機能付きコンピュータネットワーク
ホストコンピュータ
2
表示部
14
照合部
9
利用者識別子記憶部
8
端末構成情報記憶部
10
制御部
15
判定部
13
データベース
11
データベース
12
通信部
7
6 通信回線
端末装置
5
通信部
17
利用者プログラム格納部
24
利用者プログラム検索部
23
制御部
22
入出力制御部
19
構成情報記憶部
20
端末ＩＤ記憶部
21
文字入力部
16
表示部
18
フレキシブルディスク装置
3
プリンタ
4

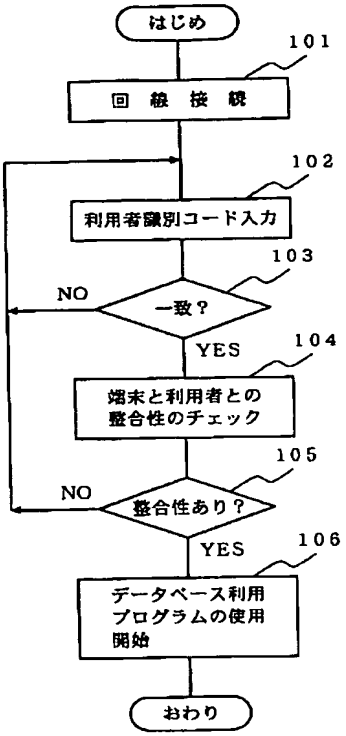
【図５】


開　始
通信要求
A1
利用者識別子要求
A2
利用者識別子入力要求
A3
利用者識別子送信
A4
利用者識別子照合
A5
不一致
一致
構成情報要求
A6
利用者プログラムの検索
B1
構成情報送信
B2
構成情報照合
B3
不一致
構成変更を通知
B4
一致
端末装置５との通信を切断
A7
アクセス権判定
B5
データベース１１
アクセス可能
B6
データベース１１，１２
アクセス可能
B7
終　了

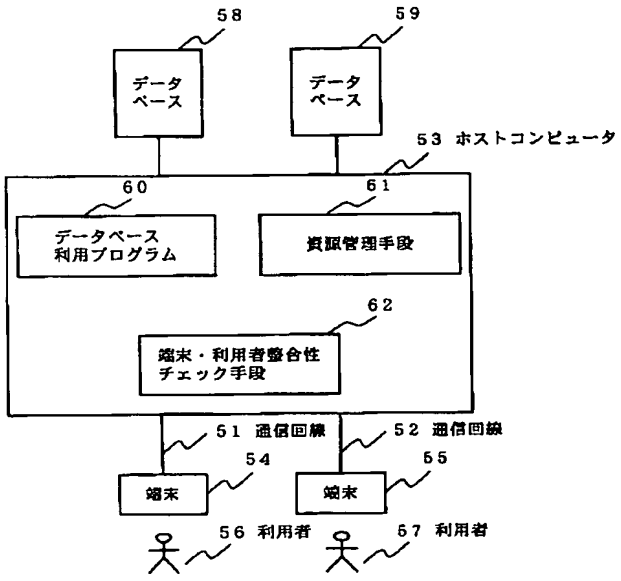
【図６】



【図８】



【図７】



【手続補正書】
【提出日】平成１１年７月２日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】端末装置には該端末装置の端末構成情報を記憶し、また該端末装置が接続されるホストコンピュータには端末装置ごとの利用者識別子と、前記端末装置に固有な情報である端末ＩＤと、前記端末装置の入出力機器を示す周辺機器の接続について情報である端末構成情報とを記憶しておき、通信要求を受信したホストコンピュータは、当該端末装置から受信した利用者識別子および端末ＩＤと自らが記憶している利用者識別子および端

末構成情報を取得し記憶しておいた前記端末構成情報と照合し一致すると、当該端末装置に対してデータベースへのアクセスの許否を判定するようにしたことを特徴とする機密情報漏洩防止機能付きコンピュータネットワーク。

【請求項２】前記端末構成情報は、前記端末装置がフレキシブルディスク装置やプリンタ装置が接続されているか否かを示す情報であることを特徴とする請求項１記載の機密情報漏洩防止機能付きコンピュータネットワーク。

【請求項３】前記端末装置は、前記利用者識別子のうちの端末ＩＤを記憶している端末ＩＤ記憶部と、前記端末構成情報を記憶している構成情報記憶とを有し、
また、前記ホストコンピュータは、前記端末ＩＤ，利用者ＩＤおよびパスワードを含む利用者識別子を記憶している利用者識別子記憶部と、前記端末ＩＤごとに前記入出力機器の有無を示す端末構成情報を記憶している端末構成情報記憶部と、前記利用者識別子および前記端末構成情報の照合を行う照合部と、該照合の結果により一致したときに当該端末装置の各入出力機器に対するデータベースごとのアクセス権の有無を判定する判定部とを有することを特徴とする請求項２記載の機密情報漏洩防止機能付きコンピュータネットワーク。

【請求項４】前記端末構成情報は、前記端末装置に格納された利用者プログラムを示す情報であり、
前記端末装置は、前記利用者識別子のうちの端末ＩＤを記憶している端末ＩＤ記憶部と、前記利用者プログラムを格納する利用者プログラム格納部と、前記ホストコンピュータから要求されると前記利用者プログラム格納部を検索する利用者プログラム検索部とを有し、
また、前記ホストコンピュータは、前記端末ＩＤ，利用者ＩＤおよびパスワードを含む利用者識別子を記憶している利用者識別子記憶部と、前記端末ＩＤごとに前記利用者プログラムの有無を示す端末構成情報を記憶している端末構成情報記憶部と、前記利用者識別子および前記端末構成情報の照合を行う照合部と、該照合の結果により一致したときに当該端末装置の各利用者プログラムに対するデータベースごとのアクセス権の有無を判定する判定部とを有することを特徴とする請求項１記載の機密情報漏洩防止機能付きコンピュータネットワーク。

【手続補正書】
【提出日】平成１１年９月１０日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】端末装置には該端末装置の端末構成情報を記憶し、また該端末装置が接続されるホストコンピュータには端末装置ごとの利用者識別子と、前記端末装置に固有な情報である端末ＩＤと、前記端末装置の入出力機器を示す周辺機器の接続についての情報である端末構成情報とを記憶しておき、通信要求を受信したホストコンピュータは、当該端末装置から受信した利用者識別子および端末ＩＤと自らが記憶している利用者識別子および端末ＩＤとを照合して一致したとき、前記端末装置から端末構成情報を取得し記憶しておいた前記端末構成情報と照合し一致すると、当該端末装置に対してデータベースへのアクセスの許否を判定するようにしたことを特徴とする機密情報漏洩防止機能付きコンピュータネットワーク。

【請求項２】前記端末構成情報は、前記端末装置がフレキシブルディスク装置やプリンタ装置が接続されているか否かを示す情報であることを特徴とする請求項１記載の機密情報漏洩防止機能付きコンピュータネットワーク。

【請求項３】前記端末装置は、前記利用者識別子のうちの端末ＩＤを記憶している端末ＩＤ記憶部と、前記端末構成情報を記憶している構成情報記憶とを有し、
また、前記ホストコンピュータは、前記端末ＩＤ，利用者ＩＤおよびパスワードを含む利用者識別子を記憶している利用者識別子記憶部と、前記端末ＩＤごとに前記入出力機器の有無を示す端末構成情報を記憶している端末構成情報記憶部と、前記利用者識別子および前記端末構成情報の照合を行う照合部と、該照合の結果により一致したときに当該端末装置の各入出力機器に対するデータベースごとのアクセス権の有無を判定する判定部とを有することを特徴とする請求項２記載の機密情報漏洩防止機能付きコンピュータネットワーク。

【請求項４】端末装置には該端末装置の端末構成情報を記憶し、また該端末装置が接続されるホストコンピュータには端末装置ごとの利用者識別子と、前記端末装置に固有な情報である端末ＩＤと、前記端末装置の利用者プログラムについての情報である端末構成情報とを記憶しておき、通信要求を受信したホストコンピュータは、当該端末装置から受信した利用者識別子および端末ＩＤと自らが記憶している利用者識別子および端末ＩＤとを照合して一致したとき、前記端末装置から端末構成情報を取得し記憶しておいた前記端末構成情報と照合し一致すると、当該端末装置に対してデータベースへのアクセスの許否を判定する機密情報漏洩防止機能付きコンピュータネットワークにおいて、
前記端末装置は、前記利用者識別子のうちの端末ＩＤを

を格納する利用者プログラム格納部と、前記ホストコンピュータから要求されると前記利用者プログラム格納部を検索する利用者プログラム検索部とを有し、
また、前記ホストコンピュータは、前記端末ＩＤ，利用者ＩＤおよびパスワードを含む利用者識別子を記憶している利用者識別子記憶部と、前記端末ＩＤごとに前記利用者プログラムの有無を示す端末構成情報を記憶している端末構成情報記憶部と、前記利用者識別子および前記端末構成情報の照合を行う照合部と、該照合の結果により一致したときに当該端末装置の各利用者プログラムに対するデータベースごとのアクセス権の有無を判定する判定部とを有することを特徴とする機密情報漏洩防止機能付きコンピュータネットワーク。